AMENDED IN SENATE JUNE 9, 2008

CALIFORNIA LEGISLATURE—2007–08 REGULAR SESSION

ASSEMBLY BILL No. 1779

Introduced by Assembly Member Jones
(Principal coauthor: Senator Torlakson)
(Coauthors: Assembly Members Adams, Aghazarian, DeSaulnier, Fuentes, Garrick, Huffman, Krekorian, and Plescia)
(Coauthors: Senators Denham, Scott, and Wyland)

January 15, 2008

An act to amend Sections 1798.29 and 1798.82 of, *and to add Sections 1724.4 and 1724.5 to,* the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

AB 1779, as amended, Jones. Personal information: security breaches.

(1) Existing law imposes specified duties upon certain persons or businesses that conduct business in California to, among other things, take reasonable steps to destroy customer records, implement and maintain reasonable security measures, disclose a breach of computerized data, and, upon request, provide specified information to a customer in relation to the disclosure of personal information to 3rd parties. For a violation of any of the above-described provisions, existing law allows an injured customer to institute a civil action to recover damages or for injunctive relief.

This bill would prohibit a person, business, or agency, as defined, that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from storing, retaining, sending, or failing to limit access to payment-related data, as defined, retaining a primary account number, or storing

sensitive authentication data subsequent to an authorization, as specified, unless a specified exception applies.

(2) Existing law requires any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require that notification to the owner or licensee of the information to include, among other things, a description of the categories of personal information that were, or may have been, acquired, a toll-free or local telephone number or electronic mail address that individuals may use to contact the agency, person, or business, and the telephone numbers and addresses of the major credit reporting agencies. If the owner or licensee of the information is the issuer of the credit or debit card or the payment device, or maintains the account from which the payment device orders payment, the bill would require the owner or licensee to disclose the same information to the California resident in plain language, as specified. The bill would also apply specified reimbursement provisions.

~~Existing~~

(3) Existing law requires any state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose any breach of the security of that data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law allows for that disclosure by written notice, electronic notice, or, upon a specified condition, by substitute notice, which, if utilized, also requires notification to major statewide media.

This bill, if substitute notice is utilized, would require that notice to also be provided to the Office of *Information Security and* Privacy Protection.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1724.4 is added to the Civil Code, to read:

1724.4. (a) In addition to being subject to the provisions of Title 1.81 (commencing with Section 1798.80) of Part 4, a person, business, or agency, as defined in subdivision (b) of Section 1798.3, that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device shall not do any of the following:

(1) Store payment-related data, except when the person, business, or agency complies with both of the following:

(A) The person, business, or agency shall have a payment data retention and disposal policy that limits the amount of payment-related data and the time that data is retained to only the amount and time required for business, legal, or regulatory purposes as explicitly documented in the policy.

(B) The person, business, or agency shall retain payment-related data only for a time period and in a manner explicitly permitted by the policy.

(2) Store sensitive authentication data subsequent to authorization, even if that data is encrypted. Sensitive authentication data includes, but is not limited to, all of the following:

(A) The full contents of any data track from a payment card or other payment device.

(B) The card verification code or any value used to verify transactions when the payment device is not present.

(C) The personal identification number (PIN) or the encrypted PIN block.

(3) Store any payment-related data that is not needed for business, legal, or regulatory purposes.

(4) Store any of the following data elements:

(A) Payment verification code.

(B) Payment verification value.

(C) PIN verification value.

(5) Retain the primary account number unless retained in a manner consistent with the other requirements of this subdivision and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored.

(6) Send payment-related data over open, public networks unless the data is encrypted using strong cryptography and security protocols or otherwise rendered indecipherable.

(7) Fail to limit access to payment-related data to only those individuals whose job requires that access.

(b) (1) This section shall not apply to any person or business subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person or business is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

(2) Nothing in this section shall prohibit a person, business, or agency, as defined in subdivision (b) of Section 1798.3, that sells goods or services to any California resident and accepts as payment a credit card, debit card, or other payment device from storing payment-related data for the sole purpose of processing ongoing or recurring payments, provided that the payment-related data is maintained in accordance with this section.

(c) For purposes of this section, "payment-related data" means any computerized information described in paragraph (3) of subdivision (e) of Section 1798.82, whether individually or in combination with any other information described in that paragraph.

SEC. 2. Section 1724.5 is added to the Civil Code, to read:

1724.5. (a) Any person, business, or agency subject to Section 1724.4 that is required to give notice of a breach of the security of the system pursuant to subdivision (b) of Section 1798.29 or subdivision (b) of Section 1798.82 shall include in that notification to the owner or licensee of the information, in plain language, all of the following information if available at the time the notice is provided:

(1) The date of the notice.

(2) The name of the agency, person, or business that maintained the computerized data at the time of the breach.

(3) The date, estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided.

(4) A description of the categories of personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

(5) A toll-free telephone number for the agency, person, or business subject to the breach of the security of the system of that agency, person, or business or, if the primary method used by that

agency, person, or business to communicate with the individuals whose information is the subject of the breach is by electronic means, an electronic mail address that the individuals may use to contact the agency, person, or business so that the individuals may learn what types of personal information that agency, person, or business maintained about the individuals were subject to the security breach. If the agency, person, or business that experienced the breach does not have a toll-free telephone number, a local telephone number may be provided to the owner or licensee of the information to contact the agency, person, or business.

(6) The toll-free telephone numbers and addresses for the major credit reporting agencies.

(b) The notification required by subdivision (a) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by subdivision (a) shall be made after the law enforcement agency determines that it will not compromise the investigation.

(c) If the owner or licensee of the information is the issuer of the credit or debit card or the payment device, or maintains the account from which the payment device orders payment, the owner or licensee shall disclose to the California resident in any notification provided pursuant to subdivision (a) of Section 1798.29 or subdivision (a) of Section 1798.82, in plain language, all information described in paragraphs (1) to (6), inclusive, of subdivision (a) of this section that is available at the time that notification is made, except however, with respect to paragraph (5), an electronic mail address may be provided in lieu of a toll-free or local telephone number to those individuals with whom the primary method used by that agency, person, or business to communicate is by electronic means.

(d) (1) Any person, business, or agency subject to Section 1724.4 required to give the notice described in subdivision (a) shall be liable to the owner or licensee of the information for the actual costs of any consumer notification provided by the owner or licensee pursuant to Section 1798.29 or 1798.82.

(2) If the person, business, or agency processes more than six million payment card transactions per year, the person, business, or agency shall additionally be liable to the owner or licensee of the information for the actual costs of reissuing the credit card, debit card, or other device upon which payment is drawn, not to

exceed the amount of fifteen dollars ($15) per reissued credit card, debit card or other payment device.

(3) A person, business, or agency subject to Section 1724.4 shall be exempt from provision (2) of this subdivision if the person, business, or agency can demonstrate compliance with the provisions of Section 1724.4 at the time the breach of security of the system occurred.

~~SECTION 1.~~

SEC. 3. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of *Information Security and* Privacy Protection.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

~~SEC. 2.~~

SEC. 4. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith

acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business

does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media and the Office of *Information Security and* Privacy Protection.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

O